Formal Analysis of Security Protocols
(Group: Crypto)

Presented by : Shruti Biswal

AERE/COMS 507X

April 11, 2017

Project Completed So Far

- Study about different security protocols : **24 Mar**
  - Needham Schroeder Public Key Protocol
  - Kerberos Protocol
  - Otway Rees Protocol
  - Neuman Stubblebine protocol
  - Yahalom protocol
- Identify states and transitions and model Needham Schroeder Public Key Protocol in NuXmv : **31 Mar**
- Validate the model and add Intruder in the model to identify possible attack : **7 Apr**
- Model Otway-Rees Protocol in NuXmv and add Intruder to identify a possible attack : **9 Apr**

Report Format

[Format]

1. Introduction : Choice of Project / Challenges / Plan of Action
2. Background Details : About different protocols
3. Analysis and Design :
   1. Protocol 1 : Identification of states and transitions / Validatory specifications
   2. Protocol 2 : Identification of states and transitions / Validatory specifications
4. Implementation : Platform / Hardware used.
5. Tests and Results:
   1. Protocol 1 : Attack (Trace) / Violated specifications
   2. Protocol 2 : Attack (Trace) / Violated specifications
6. Conclusion
7. Bibliography
8. Appendix : Model/Code

Challenges & Plan of Action

Challenges	Plan of Action
Interaction among the agents in a protocol gets complicated with the size of message being exchanged as per current design.	Re-model the agents with only incoming messages, if time permits Consider this for the models yet to be completed.
Kerberos Protocol has a KDC, that generates authenticated unique tickets with a lifetime. Most time taking, so far.	Modelling the KDC as an agent simplified the situation. Plan to generate unique tickets by use of time-stamp. For lifetime of a ticket, either make it dependent on the state of agent or, compare with the actual time elapsed after generation.

Expected Changes

- The result analysis in the proposal stated to compare the time taken by different algorithms for detection of the attacks. So far there has been no significant difference. Hence, I plan to include a causal analysis of the attacks in the protocols.
- The aim is to complete the implementation part of project as stated in the proposal.
- However, given the complexity and size of the Kerberos Protocol, incase of inability to model this protocol, I plan to model some other small-size security protocols as part of compensation :
  - Neuman Stubblebine protocol
  - Yaholom Protocol